Guía de configuración de IPsec

Versión 0

SPA

Definiciones de las notas

A lo largo de esta guía del usuario se utiliza el siguiente icono:

Nota	Las notas indican cómo responder ante situaciones que pueden presentarse, o bien ofrecen consejos sobre cómo funcionará la operación con otras funciones.

Marcas comerciales

El logotipo de Brother es una marca comercial registrada de Brother Industries, Ltd.

Todos los nombres comerciales y nombres de productos de empresas que aparecen en productos Brother, documentos asociados y cualquier otro material son marcas comerciales o marcas comerciales registradas de estas respectivas empresas.

©2012 Brother Industries, Ltd. Todos los derechos reservados.

Tabla de contenido

1 Introducción 1

Descripción general 1
Configuración mediante Administración basada en Web (navegador web) 2

2 Ajustes de IPsec 5

Plantilla de dirección 5
Plantilla de servicio 7
Plantilla de servicio IPsec 7
Configuración de un servicio 9
Plantilla IPsec 11

A Apéndice A 20

Plantillas de servicio 20
Tipo/Código 21

1 Introducción

Descripción general

IPsec (Protocolo de seguridad de Internet) es un protocolo de seguridad que utiliza una función de protocolo de Internet para evitar la manipulación y asegurar la confidencialidad de los datos transmitidos como paquetes IP. IPsec cifra datos transmitidos por la red, como los datos enviados desde los ordenadores (computadoras) a una impresora. Como los datos están cifrados en el nivel de red, las aplicaciones que utilizan un protocolo de mayor nivel usan IPsec incluso cuando el usuario no es consciente de su uso.

IPsec admite las siguientes funciones:

■ Transmisiones IPsec

Según las condiciones de los ajustes de IPsec, el ordenador conectado a la red envía datos y los recibe desde el dispositivo especificado mediante IPsec. Cuando los dispositivos inician la comunicación mediante IPsec, las teclas se intercambian primero mediante IKE (Intercambio de claves por red) y, a continuación, los datos se transmiten por medio de las claves.

Además, IPsec tiene dos modos de operación: el modo de transporte y el modo de túnel. El modo de transporte se utiliza principalmente para establecer la comunicación entre dispositivos, mientras que el modo de túnel se utiliza como una VPN (Red privada virtual).

Nota

- En las transmisiones IPsec son necesarias las siguientes condiciones:
  - Que un ordenador que pueda comunicarse con IPsec esté conectado a la red.
  - Que la impresora o el equipo MFC esté configurado para establecer la comunicación IPsec.
  - Que el ordenador conectado a la impresora o al equipo MFC esté configurado para establecer conexiones IPsec.
- IPsec no admite comunicación de difusión o multidifusión.

■ Ajustes de IPsec

Son los ajustes necesarios para establecer conexiones mediante IPsec. Estos ajustes pueden configurarse mediante Administración basada en Web. (Consulte *Configuración mediante Administración basada en Web (navegador web)* ➤➤ página 2).

Nota

Para configurar los ajustes de IPsec, es necesario que esté conectado a la red un ordenador desde el que se pueda controlar el navegador.

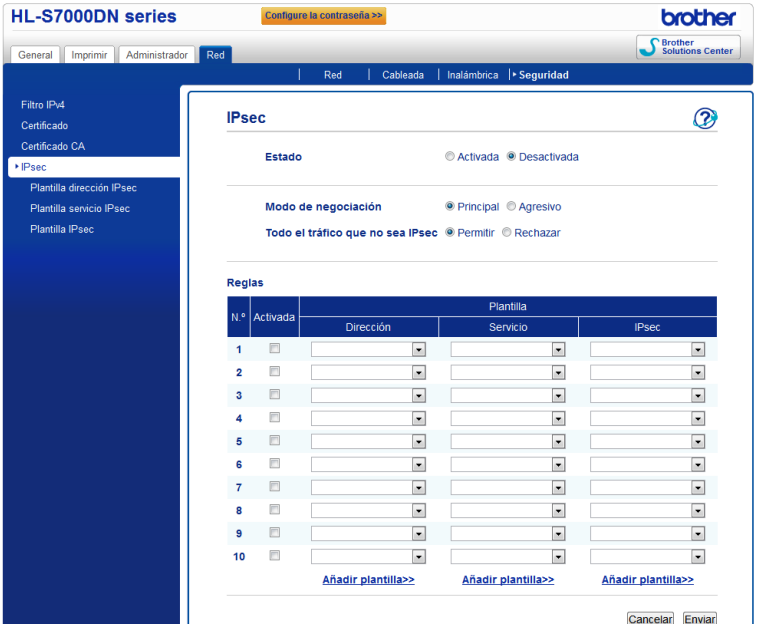
Configuración mediante Administración basada en Web (navegador web)

Utilice la pantalla de ajustes de IPsec en Administración basada en Web para especificar las condiciones de conexión de IPsec.

Las condiciones de conexión de IPsec se dividen en tres tipos de **Plantilla**: **Dirección**, **Servicio** e **IPsec**; además, se pueden configurar un máximo de 10 condiciones de conexión.

1. Inicie el navegador web.
2. Introduzca “http://dirección IP del equipo/” en el navegador (“dirección IP del equipo” es la dirección IP del equipo).
   - Por ejemplo:

     http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Introduzca una contraseña si ha establecido una y pulse .
4. Haga clic en la pestaña **Red**.
5. Haga clic en **Seguridad**.
6. Haga clic en **IPsec**.
7. Es posible configurar los ajustes de IPsec desde la pantalla indicada a continuación.



- **Estado**

  Seleccione **Activada** o **Desactivada** para IPsec.
- **Modo de negociación**

  Seleccione el modo de la Fase 1 de IKE.

- **Principal**: se utiliza el modo principal.
- **Agresivo**: se utiliza el modo agresivo.

Nota

IKE es un protocolo que se utiliza para intercambiar claves de cifrado para llevar a cabo una comunicación cifrada mediante IPsec.

Si el modo **Principal** está seleccionado, la velocidad de procesamiento es baja pero la seguridad es alta. Si el modo **Agresivo** está seleccionado, la velocidad de procesamiento es mayor que cuando se selecciona el modo **Principal**, pero la seguridad es menor.

■ **Todo el tráfico que no sea IPsec**

Seleccione la acción que se realizará en paquetes que no sean IPsec.

- **Permitir**: permite que se reciban todos los paquetes.
- **Rechazar**: descarta todos los paquetes que no sean IPsec.

Nota

Cuando utilice Web services (Servicios web), debe seleccionar **Permitir** en **Todo el tráfico que no sea IPsec**. Si **Rechazar** está seleccionado, no se podrá utilizar Web services (Servicios web).

■ **Reglas**

Se pueden configurar un máximo de 10 condiciones de conexión de IPsec (conjunto de plantillas).

■ **Activada**

Cuando se selecciona esta casilla de verificación, se habilita el conjunto de plantilla para tal número.

Nota

Cuando se seleccionan varias casillas de verificación y si existe un conflicto entre las casillas de verificación seleccionadas, tienen prioridad las casillas de verificación con los números más bajos.

■ **Plantilla** - **Dirección**

Seleccione la **Plantilla de dirección** que se utilizará para las condiciones de conexión de IPsec.

Para añadir una **Plantilla de dirección**, haga clic en **Añadir plantilla**. (Consulte *Plantilla de dirección* ➤➤ página 5).

■ **Plantilla** - **Servicio**

Seleccione la **Plantilla de servicio** que se utilizará para las condiciones de conexión de IPsec.

Para añadir una **Plantilla de servicio**, haga clic en **Añadir plantilla**. (Consulte *Plantilla de servicio* ➤➤ página 7).

Nota

Si desea utilizar DNS para la resolución del nombre cuando utilice las plantillas de servicio 2, 3 y 4 del *Apéndice A*, los ajustes de DNS tienen que ser configurados por separado.

■ **Plantilla** - **IPsec**

Seleccione la **Plantilla IPsec** que se utilizará para las condiciones de conexión de IPsec.

Para añadir una **Plantilla IPsec**, haga clic en **Añadir plantilla**. (Consulte *Plantilla IPsec* ➤➤ página 11).

■ **Enviar**

Haga clic en este botón para registrar los ajustes. Si el ordenador tiene que reiniciarse para cambiar los ajustes, se mostrará una pantalla de confirmación de reinicio cuando se haga clic en este botón.

Nota

Si seleccione la casilla de verificación **Activada** y hace clic en **Enviar**, se producirá un error si hay un elemento en blanco en la plantilla seleccionada.

2 Ajustes de IPsec

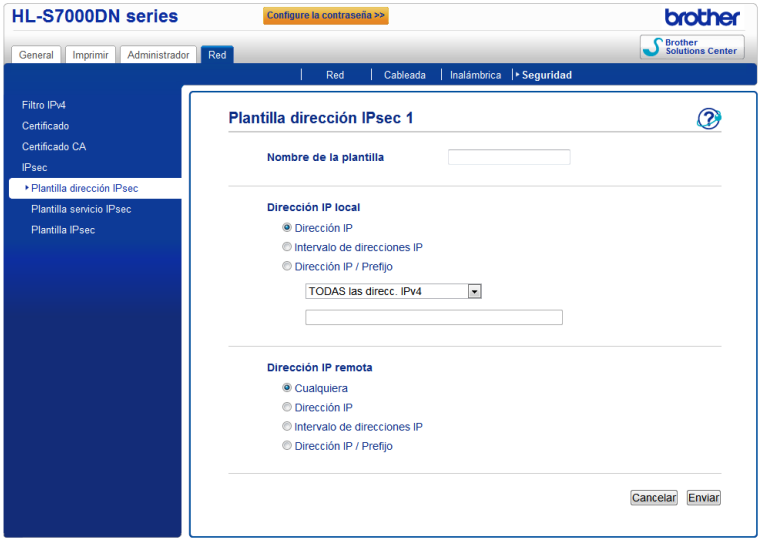
Plantilla de dirección

Especifique las direcciones IP que se usarán en las condiciones de conexión de IPsec. Se pueden utilizar un máximo de 10 tipos de **Plantilla de dirección**.

1. Inicie el navegador web.
2. Introduzca “http://dirección IP del equipo/” en el navegador (“dirección IP del equipo” es la dirección IP del equipo).
   - Por ejemplo:

     http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Introduzca una contraseña si ha establecido una y pulse .
4. Haga clic en la pestaña **Red**.
5. Haga clic en **Seguridad**.
6. Haga clic en **Plantilla dirección IPsec**.
   10 tipos de **Plantilla de dirección** serán mostrados. Si no se ha configurado **Plantilla de dirección**, se mostrará **Sin configurar**.
   - **Eliminar**

     Haga clic en este botón para eliminar la **Plantilla de dirección** seleccionada. No obstante, no se podrá eliminar la **Plantilla de dirección** actualmente en uso.
7. Haga clic en el número de la **Plantilla de dirección** que desea crear. Especifique la dirección IP que desea utilizar para IPsec en la pantalla que se muestra a continuación y cree la **Plantilla dirección IPsec**.



■ **Nombre de la plantilla**

Introduzca un nombre para la plantilla en este cuadro (16 caracteres como máximo).

■ **Dirección IP local**

Especifique las condiciones de la dirección IP del emisor.

- **Dirección IP**

  Especifique la dirección IP. Seleccione **TODAS las direcc. IPv4**, **TODAS las direcc. IPv6**, **TODOS los enlaces IPv6 locales** o **Personalizar**.

  Si se selecciona **Personalizar**, introduzca la dirección IP especificada (IPv4 o IPv6) en el cuadro de texto.

- **Intervalo de direcciones IP**

  Introduzca las direcciones IP de inicio y finalización del intervalo de direcciones IP. Si las direcciones IP de inicio y finalización no están estandarizadas a IPv4 o IPv6, o bien la dirección IP de finalización es menor que la dirección de inicio, se producirá un error.

- **Dirección IP / Prefijo**

  Especifique la dirección IP haciendo uso de un prefijo.

  Por ejemplo: 192.168.1.1/24

  Como el prefijo se especifica en la forma de una máscara de subred de 24 bits (255.255.255.0) para 192.168.1.1, las direcciones 192.168.1.xx son válidas.

■ **Dirección IP remota**

Especifique las condiciones de la dirección IP del destinatario.

- **Cualquiera**

  Cuando se selecciona **Cualquiera**, se habilitan todas las direcciones IP.

- **Dirección IP**

  Introduzca la dirección IP especificada (IPv4 o IPv6) en el cuadro de texto.

- **Intervalo de direcciones IP**

  Introduzca las direcciones IP de inicio y finalización del intervalo de direcciones IP. Si las direcciones IP de inicio y finalización no están estandarizadas a IPv4 o IPv6, o bien la dirección IP de finalización es menor que la dirección de inicio, se producirá un error.

- **Dirección IP / Prefijo**

  Especifique la dirección IP haciendo uso de un prefijo.

  Por ejemplo: 192.168.1.1/24

  Como el prefijo se especifica en la forma de una máscara de subred de 24 bits (255.255.255.0) para 192.168.1.1, las direcciones 192.168.1.xx son válidas.

■ **Enviar**

Haga clic en este botón para registrar los ajustes.

Nota

Cuando cambie los ajustes de la plantilla actualmente en uso, la pantalla de ajustes de IPsec para Administración basada en Web se cerrará y se volverá a abrir.

Plantilla de servicio

Plantilla de servicio IPsec

Especifique el protocolo y el número de puerto que desea utilizar en las conexiones IPsec. Se pueden utilizar un máximo de 10 tipos de **Plantilla de servicio**.

1. Inicie el navegador web.
2. Introduzca “http://dirección IP del equipo/” en el navegador (“dirección IP del equipo” es la dirección IP del equipo).
   - Por ejemplo:

     http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Introduzca una contraseña si ha establecido una y pulse .
4. Haga clic en la pestaña **Red**.
5. Haga clic en **Seguridad**.
6. Haga clic en **Plantilla servicio IPsec**.
   10 tipos de **Plantilla de servicio** serán mostrados. Si no se ha configurado **Plantilla de servicio**, se mostrará **Sin configurar**.
   - **Eliminar**

     Haga clic en este botón para eliminar la **Plantilla de servicio** seleccionada. No obstante, no se podrá eliminar la **Plantilla de servicio** actualmente en uso.

7 Haga clic en el número de la **Plantilla de servicio** que desea crear. Seleccione los servicios que desea utilizar para IPsec en la pantalla que se muestra a continuación y cree la **Plantilla servicio IPsec**. Además, si desea crear servicios originales, haga clic en **Configurar servicio**. (Consulte *Configuración de un servicio* ➤➤ página 9).

■ **Nombre de la plantilla**

Introduzca un nombre para la plantilla en este cuadro (16 caracteres como máximo).

■ **Nombre del servicio**

Se muestran los nombres de los servicios predeterminados y los nombres de los servicios previamente creados. Seleccione los servicios que desea añadir a la plantilla.

■ **Configurar servicio**

Haga clic en **Configurar servicio** para configurar la plantilla mediante la adición de servicios. (Consulte *Configuración de un servicio* ➤➤ página 9).

■ **Servicio seleccionado**

Se muestra la información del servicio (**Nombre del servicio**, **Dirección**, **Protocolo** y **Puerto**) que se ha seleccionado en **Nombre del servicio**.

Nota

- Se puede añadir un máximo de 32 servicios a la vez.
- Para obtener más detalles sobre los protocolos que puede especificar en **Plantilla servicio IPsec**, consulte *Apéndice A*.

■ **Enviar**

Haga clic en este botón para registrar los ajustes.

Nota

Cuando cambie los ajustes de la plantilla actualmente en uso, la pantalla de ajustes de IPsec para Administración basada en Web se cerrará y se volverá a abrir.

Configuración de un servicio

Cree un nuevo servicio.

1. En la pantalla **Plantilla servicio IPsec**, haga clic en **Configurar servicio**.
   60 tipos de **Nombre del servicio** serán mostrados. Si no se ha configurado **Nombre del servicio**, se mostrará **Sin configurar**.

   - **Eliminar**

     Haga clic en este botón para eliminar el **Nombre del servicio** seleccionado. No obstante, no se podrá eliminar el **Nombre del servicio** actualmente en uso.

   - **Plantilla servicio IPsec**

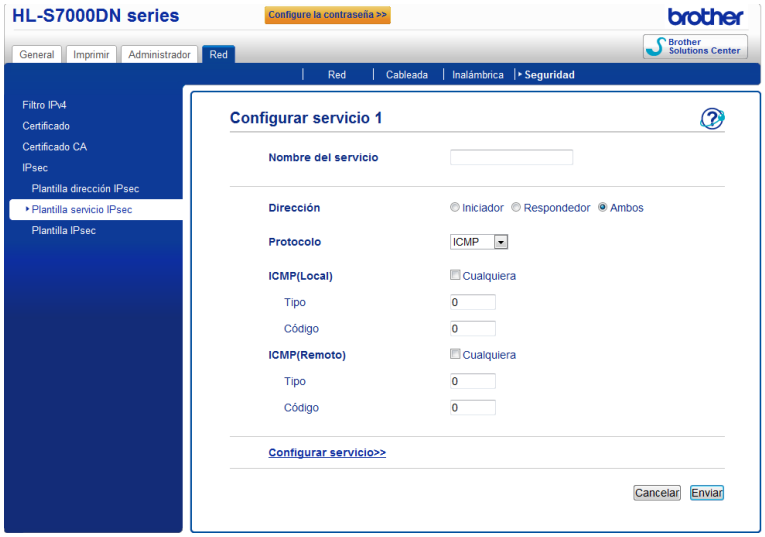
     Haga clic en este botón para volver a la pantalla **Plantilla servicio IPsec**.

2. Haga clic en el número del **Nombre del servicio** que desea crear. Seleccione los servicios que desea utilizar para IPsec en la pantalla indicada a continuación. Los elementos de ajuste varían en función del **Protocolo** seleccionado.

(**Protocolo**:**TODOS**)

(**Protocolo**:**TCP** o **UDP**)

(**Protocolo**: **ICMP**)



■ **Nombre del servicio**

Introduzca un nombre para el servicio en este cuadro (16 caracteres como máximo).

■ **Dirección**

Especifique la dirección de la comunicación. Seleccione **Iniciador**, **Respondedor** o **Ambos**.

■ **Protocolo**

Especifique el protocolo que está habilitado. Seleccione **TODOS**, **TCP**, **UDP** o **ICMP**. Los elementos de ajuste varían en función del **Protocolo** seleccionado.

- Cuando esté seleccionado **TCP** o **UDP**, registre el **Puerto local**/**Puerto remoto**.
- Cuando esté seleccionado **ICMP**, registre el **Tipo**/**Código**.

Nota

ICMP es un protocolo que se utiliza para enviar mensajes de control y mensajes de error IP. Este protocolo es utilizado por ordenadores y dispositivos de red conectados mediante TCP/IP para llevar a cabo una confirmación de estado mutua.

- **Puerto local/Puerto remoto** (cuando **TCP** o **UDP** se selecciona en **Protocolo**).

  Introduzca un número de puerto local. Si **Único** está seleccionado, introduzca un número de puerto. Si está seleccionado **Intervalo**, introduzca el número de puerto de inicio y, a continuación, el número de puerto de finalización. Cuando desee habilitar todos los números de puerto, seleccione **Intervalo** e introduzca “1-65535” sin las comillas.

- **ICMP(Local)/ICMP(Remoto)** (cuando **ICMP** se selecciona en **Protocolo**).

  Configure los ajustes de ICMP. Seleccione **Cualquiera** o introduzca **Tipo**/**Código**. Para obtener más detalles sobre **Tipo**/**Código**, consulte *Apéndice A*.

- **Configurar servicio**

  Haga clic en este botón para volver a la pantalla **Configurar servicio**.

- **Enviar**

  Haga clic en este botón para registrar los ajustes.

Nota

Cuando cambie los ajustes de la plantilla actualmente en uso, la pantalla de ajustes de IPsec para Administración basada en Web se cerrará y se volverá a abrir.

Plantilla IPsec

Configure los ajustes de IKE/IPsec. Se pueden utilizar un máximo de 10 tipos de **Plantilla IPsec**.

1. Inicie el navegador web.
2. Introduzca “http://dirección IP del equipo/” en el navegador (“dirección IP del equipo” es la dirección IP del equipo).
   - Por ejemplo:

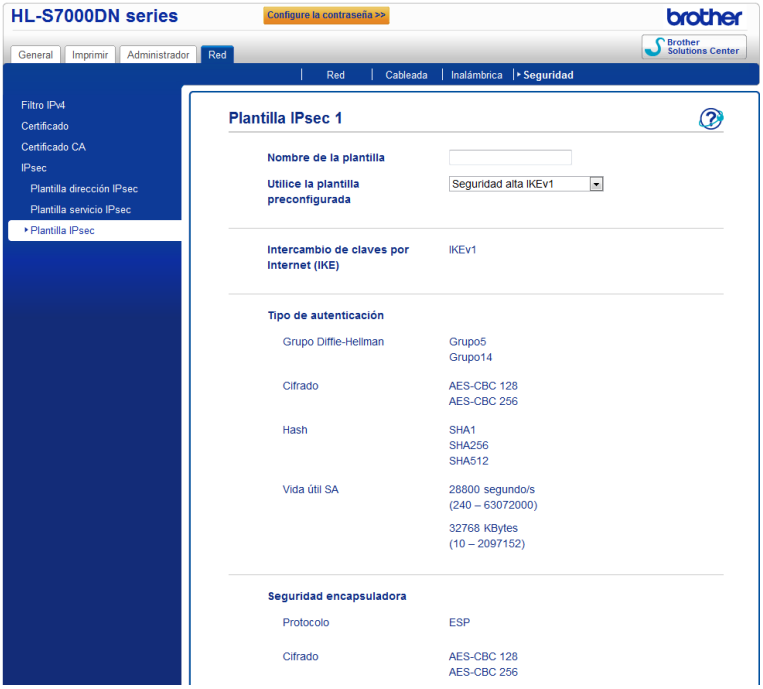
     http://192.168.1.2/
3. No se necesita una contraseña de manera predeterminada. Introduzca una contraseña si ha establecido una y pulse →.
4. Haga clic en la pestaña **Red**.
5. Haga clic en **Seguridad**.
6. Haga clic en **Plantilla IPsec**.
   10 tipos de **Plantilla IPsec** serán mostrados. Si no se ha configurado **Plantilla IPsec**, se mostrará **Sin configurar**.

Eliminar

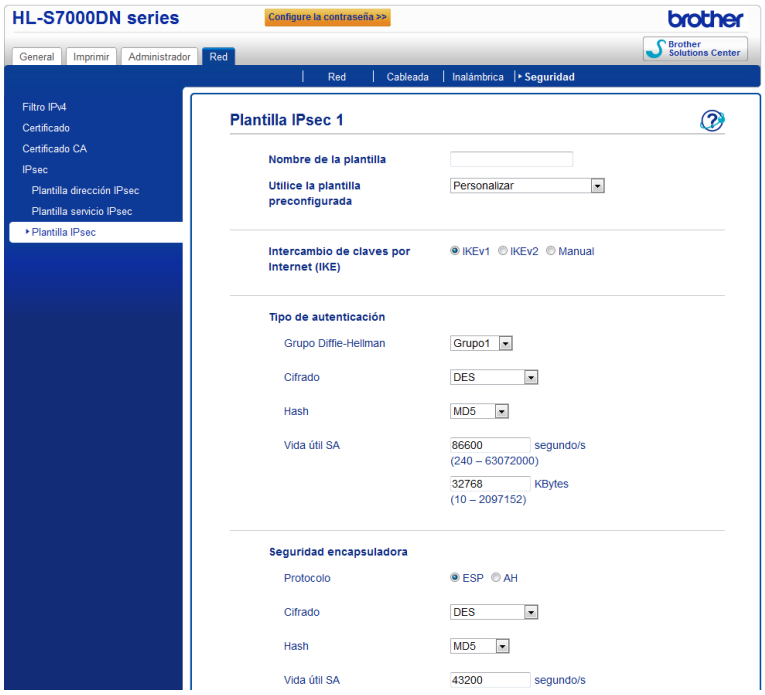
Haga clic en este botón para eliminar la **Plantilla IPsec** seleccionada. No obstante, no se podrá eliminar la **Plantilla IPsec** actualmente en uso.

7 Haga clic en el número de la **Plantilla IPsec** que desea crear. Configure los ajustes de IPsec en la pantalla indicada a continuación y cree la **Plantilla IPsec**. Los elementos de ajuste varían en función de la opciones seleccionadas en **Utilice la plantilla preconfigurada** e **Intercambio de claves por Internet (IKE)**.

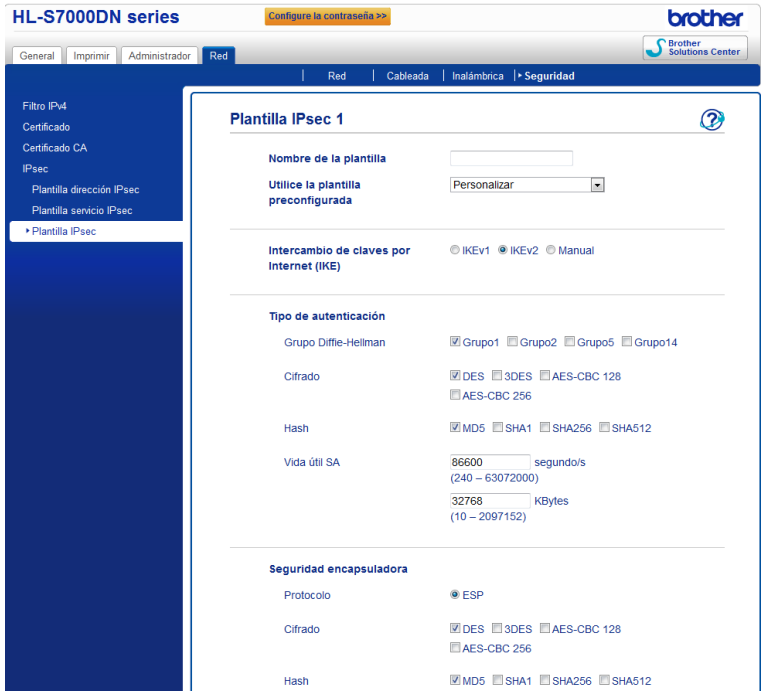
(**IKE**:**Predefinido**)



(**IKE**:**IKEv1**)



(**IKE**:**IKEv2**)



■ Nombre de la plantilla

Introduzca un nombre para la plantilla en este cuadro (16 caracteres como máximo).

■ **Utilice la plantilla preconfigurada**

Seleccione **Personalizar**, **Seguridad alta IKEv1**, **Seguridad media IKEv1**, **Seguridad alta IKEv2** o **Seguridad media IKEv2**. Los elementos de ajuste varían en función de la plantilla seleccionada.

Nota

La plantilla predeterminada difiere dependiendo de si selecciona el modo de negociación como principal o como agresivo en la pantalla de ajustes de IPsec. Para obtener más detalles sobre la pantalla de ajustes de IPsec, consulte *Configuración mediante Administración basada en Web (navegador web)* ➤➤ página 2.

■ **Intercambio de claves por Internet (IKE)**

IKE es un protocolo de comunicación que se utiliza para intercambiar claves de cifrado para llevar a cabo una comunicación cifrada mediante IPsec. Para realizar la comunicación cifrada solo por una vez, se determina el algoritmo de cifrado necesario para IPsec y se comparten las claves de cifrado. Para IKE, las claves de cifrado se intercambian mediante el método de intercambio de claves Diffie-Hellman y se lleva a cabo la comunicación cifrada limitada a IKE.

Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada**, seleccione **IKEv1**, **IKEv2** o **Manual**.

Si está seleccionado un ajuste que no sea **Personalizar**, se mostrará el tipo de ajuste seleccionado en **Utilice la plantilla preconfigurada**.

■ **Tipo de autenticación**

Configura el cifrado y la autenticación IKE.

- **Grupo Diffie-Hellman**

  Este método de intercambio de claves permite que las claves secretas se intercambien con seguridad en una red desprotegida. El método de intercambio de claves Diffie-Hellman utiliza un problema de logaritmos discretos, en vez de una clave secreta, para enviar y recibir información abierta que ha sido generada mediante un número aleatorio y la clave secreta.

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **IKEv1** o **IKEv2** está seleccionado en **IKE**), seleccione **Grupo1**, **Grupo2**, **Grupo5** o **Grupo14**. Si se selecciona **IKEv2**, son posibles varias selecciones.

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **Manual** está seleccionado en **IKE**), no se mostrará el grupo.

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el grupo habilitado que se ha mencionado anteriormente.

- **Cifrado**

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **IKEv1** o **IKEv2** está seleccionado en **IKE**), seleccione **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. Si se selecciona **IKEv2**, son posibles varias selecciones.

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **Manual** está seleccionado en **IKE**), no se mostrará el cifrado.

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el cifrado habilitado que se ha mencionado anteriormente.

- **Hash**

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **IKEv1** o **IKEv2** está seleccionado en **IKE**), seleccione **MD5**, **SHA1**, **SHA256** o **SHA512**. Si se selecciona **IKEv2**, son posibles varias selecciones.

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **Manual** está seleccionado en **IKE**), no se mostrará el tipo de algoritmo de hash.

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el tipo de algoritmo de hash habilitado que se ha mencionado anteriormente.

- **Vida útil SA**

  Especifique la vida útil de IKE SA.

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **IKEv1** o **IKEv2** está seleccionado en **IKE**), introduzca el tiempo (segundos) y el número de kilobytes (KByte).

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **Manual** está seleccionado en **IKE**), no se mostrará la información de la vida útil SA.

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el tiempo (segundos) y el número de kilobytes (KByte).

■ **Seguridad encapsuladora**

- **Protocolo**

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada**), seleccione **ESP** o **AH**. Si se selecciona **IKEv2** en **IKE**, solo se puede seleccionar **ESP**.

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el protocolo habilitado que se ha mencionado anteriormente.

Nota

- ESP es un protocolo para establecer comunicación cifrada mediante IPsec. ESP cifra la carga útil (contenidos comunicados) y añade información adicional. El paquete IP consta del encabezado y de la carga útil cifrada que sigue al encabezado. Además de los datos cifrados, el paquete IP también incluye información relativa al método de cifrado y a la clase de cifrado, a los datos de autenticación, etcétera.
- AH es parte del protocolo IPsec que autentica al emisor y evita la manipulación de los datos (asegura la compleción de los datos). En el paquete IP, los datos se introducen inmediatamente después del encabezado. Además, los paquetes incluyen valores de hash, que se calculan mediante una ecuación basada en los contenidos comunicados, la clave secreta, etcétera, para evitar la falsificación del emisor y la manipulación de los datos. A diferencia de ESP, los contenidos comunicados no son cifrados y los datos se envían y se reciben como texto sin formato.

- **Cifrado**

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada**), seleccione **DES**, **3DES**, **AES-CBC 128** o **AES-CBC 256**. El cifrado solo puede seleccionarse cuando se selecciona **ESP** en **Protocolo**. Si se selecciona **IKEv2** en **IKE**, son posibles varias selecciones.

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el cifrado habilitado que se ha mencionado anteriormente.

- **Hash**

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **IKEv1** o **Manual** está seleccionado en **IKE**), seleccione **Ninguno**, **MD5**, **SHA1**, **SHA256** o **SHA512**. **Ninguno** solo puede seleccionarse cuando se seleccione **ESP** en **Protocolo**.

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **IKEv2** está seleccionado en **IKE**), seleccione **MD5**, **SHA1**, **SHA256** o **SHA512**. Son posibles varias selecciones.

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el tipo de algoritmo de hash habilitado que se ha mencionado anteriormente.

- **Vida útil SA**

  Especifique la vida útil de IKE SA.

  (Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **IKEv1** o **IKEv2** está seleccionado en **IKE**), introduzca el tiempo (segundos) y el número de kilobytes (KByte).

  (Si está seleccionado un ajuste que no sea **Personalizar** en **Utilice la plantilla preconfigurada**), se mostrará el tiempo (segundos) y el número de kilobytes (KByte).

- **Modo de encapsulación**

  Seleccione **Transporte** o **Túnel**.

- **Dirección IP router remoto**

  Especifique la dirección IP (IPv4 o IPv6) del destino de conexión. Introdúzcalo solo cuando se seleccione el modo de **Túnel**.

Nota

SA (Asociación de seguridad) es un método de comunicación cifrada mediante IPsec o IPv6 que intercambia y comparte información, como el método de cifrado y la clave de cifrado para establecer un canal de comunicación de seguridad antes de que se inicie la comunicación. Es posible que SA también haga referencia a un canal de comunicación cifrada virtual que se ha establecido. La SA utilizada para IPsec establece un método de cifrado, intercambia las claves y realiza una autenticación según el procedimiento IKE (Intercambio de claves por red) estándar. Además, la SA se actualiza automáticamente.

■ **Confidencialidad directa perfecta (PFS)**

PFS no obtiene claves a partir de claves previas que han sido utilizadas para cifrar mensajes. Además, si una clave que ha utilizado para cifrar un mensaje se ha obtenido a partir de una clave primaria, tal clave primaria no se utiliza para obtener otras claves. Por lo tanto, incluso si una clave está en riesgo, el daño se limitará solo a los mensajes que han sido cifrados utilizando dicha clave.

Seleccione **Activada** o **Desactivada**. Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **Manual** está seleccionado en **IKE**, no se mostrará la información PFS.

■ **Método de autentificación**

Seleccione el método de autenticación. Seleccione **Clave precompartida**, **Certificados**, **EAP - MD5** o **EAP - MS-CHAPv2**.

EAP - MD5 y **EAP - MS-CHAPv2** pueden seleccionarse solo cuando **IKEv2** está seleccionado en **IKE**. Si **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **Manual** está seleccionado en **IKE**, no se mostrará la información del método de autenticación.

■ **Clave precompartida**

Al cifrar la comunicación, se intercambia la clave de cifrado y se comparte primero mediante otro canal.

Si **Clave precompartida** está seleccionada en **Método de autentificación**, introduzca la **Clave precompartida** (32 caracteres como máximo).

- **Local Tipo ID/ID**

  Seleccione el tipo de ID del emisor e introduzca la ID.

  Seleccione **Dirección IPv4**, **Dirección IPv6**, **FQDN**, **Dirección de correo electrónico** o **Certificado** para el tipo de ID.

  Si **Certificado** está seleccionado, introduzca el nombre común del certificado en **ID**.

- **Remoto Tipo ID/ID**

  Seleccione el tipo de ID del destinatario e introduzca la ID.

  Seleccione **Dirección IPv4**, **Dirección IPv6**, **FQDN**, **Dirección de correo electrónico** o **Certificado** para el tipo de ID.

  Si **Certificado** está seleccionado, introduzca el nombre común del certificado en **ID**.

■ **Certificados**

Si **Certificados** está seleccionado en **Método de autentificación**, seleccione el certificado.

Nota

Solo puede seleccionar los certificados que fueron creados mediante la página **Certificado** de las funciones de seguridad de Administración basada en Web. Para obtener más detalles, consulte Guía del usuario en red: Uso de certificados para la seguridad de dispositivos.

■ **EAP**

EAP es un protocolo de autenticación que es una extensión de PPP. Al utilizar EAP junto con IEEE802.1x, se utiliza una clave diferente para la autenticación del usuario y cada una de las sesiones.

Los siguientes ajustes son necesarios solo cuando **EAP - MD5** o **EAP - MS-CHAPv2** está seleccionado en **Método de autentificación**.

- **Modo**

  Seleccione **Modo-Servidor** o **Modo-Cliente**.

- **Certificado**

  Seleccione el certificado.

- **Nombre de usuario**

  Introduzca el nombre del usuario (32 caracteres como máximo).

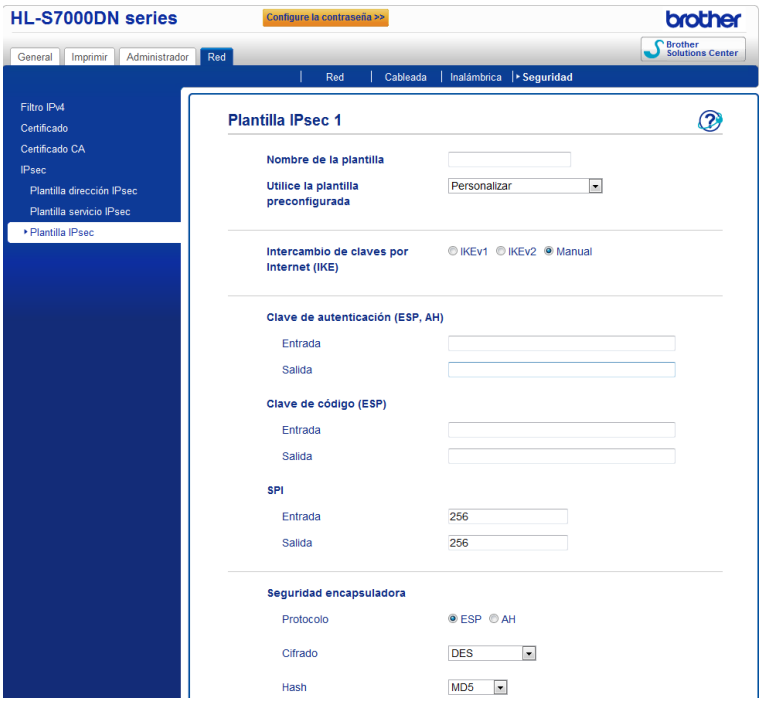
- **Contraseña**

  Introduzca la contraseña. La contraseña debe ser introducida dos veces para su confirmación (32 caracteres como máximo).

- **Certificado>>**

  Haga clic en este botón para moverse a la pantalla de ajustes del certificado.

(**IKE**:**Manual**)



■ **Clave de autenticación (ESP, AH)**

Especifique la clave que desea utilizar para la autenticación. Introduzca los valores de **Entrada**/**Salida**.

Estos ajustes son necesarios cuando **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada**, **Manual** está seleccionado en **IKE** y un ajuste que no sea **Ninguno** está seleccionado en **Hash** dentro de **Seguridad encapsuladora**.

Nota

El número de caracteres que puede establecer varía en función del ajuste que haya seleccionado en Hash dentro de Seguridad encapsuladora.

Si la longitud de la clave de autenticación especificada es diferente del algoritmo de hash seleccionado, se producirá un error.

- **MD5**: 128 bits (16 bytes)
- **SHA1**: 160 bits (20 bytes)
- **SHA256**: 256 bits (32 bytes)
- **SHA512**: 512 bits (64 bytes)

Cuando especifique la clave en código ASCII, añada comillas a los caracteres.

■ **Clave de código (ESP)**

Especifique la clave que desea utilizar para el cifrado. Introduzca los valores de **Entrada**/**Salida**.

Estos ajustes son necesarios cuando **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada**, **Manual** está seleccionado en **IKE** y **ESP** está seleccionado en **Protocolo** dentro de **Seguridad encapsuladora**.

Nota

El número de caracteres que puede establecer varía en función del ajuste que haya seleccionado en Cifrado dentro de Seguridad encapsuladora.

SI la longitud del código especificado es diferente al algoritmo de cifrado seleccionado, se producirá un error.

- **DES**: 64 bits (8 bytes)
- **3DES**: 192 bits (24 bytes)
- **AES-CBC 128**: 128 bits (16 bytes)
- **AES-CBC 256**: 256 bits (32 bytes)

Cuando especifique la clave en código ASCII, añada comillas a los caracteres.

■ **SPI**

Estos parámetros se utilizan para identificar la información de seguridad. Por lo general, un host tiene varias SA (Asociaciones de seguridad) para los distintos tipos de comunicación IPsec. Por lo tanto, es necesario identificar la SA aplicable cuando se recibe un paquete IPsec. El parámetro SPI, que identifica la SA, se incluye en el AH (Encabezado de autentificación) y el encabezado ESP (Carga útil de seguridad encapsuladora).

Estos ajustes son necesarios cuando **Personalizar** está seleccionado en **Utilice la plantilla preconfigurada** y **Manual** está seleccionado en **IKE**.

Introduzca los valores de **Entrada**/**Salida** (3-10 caracteres).

■ **Enviar**

Haga clic en este botón para registrar los ajustes.

Nota

Cuando cambie los ajustes de la plantilla actualmente en uso, la pantalla de ajustes de IPsec para Administración basada en Web se cerrará y se volverá a abrir.

A Apéndice A

Plantillas de servicio

Puede utilizar los siguientes servicios mediante la selección de las plantillas.

1 Todos los servicios

IPsec se utiliza para todos los protocolos.

2 Servicios de impresión

Nombre del servicio	Protocolo	Puerto local	Puerto remoto
IPP	TCP	631	Cualquiera
IPPS	TCP	443	Cualquiera
FTP (Control)	TCP	21	Cualquiera
FTP (Datos)	TCP	20	Cualquiera
P9100	TCP	9100	Cualquiera
Servicios web	TCP	80	Cualquiera
LPD	TCP	515	Cualquiera

3 Servicios de administración

Nombre del servicio	Protocolo	Puerto local	Puerto remoto
SNMP	UDP	161	Cualquiera
Telnet	TCP	23	Cualquiera
HTTP	TCP	80	Cualquiera
HTTPS	TCP	443	Cualquiera
Configuración remota	TCP	54922	Cualquiera

4 Servicios MFC/impresora [1]

Nombre del servicio	Protocolo	Puerto local	Puerto remoto
CIFS	TCP	Cualquiera	445
SMB	TCP	Cualquiera	139
LDAP	TCP	Cualquiera	389
SMTP	TCP	Cualquiera	25
POP3	TCP	Cualquiera	110
SNTP	UDP	Cualquiera	123
Exploración de red	TCP	54921	Cualquiera
PC-FAX	TCP	54923	Cualquiera

Nombre del servicio	Protocolo	Puerto local	Puerto remoto
Kerberos (TCP)	TCP	Cualquiera	88
Kerberos (UDP)	UDP	Cualquiera	88

[1] Si desea utilizar autenticación Kerberos, tendrá que habilitar los correspondientes ajustes DNS.

Tipo/Código

Los siguientes tipos y códigos son admitidos cuando **ICMP** está seleccionado en **Protocolo**.

IPv4		
Tipo		**Códigos admitidos**
0	Echo Reply	0
3	Destination Unreachable	0,1,2,3,4,5,6,7,8,9,10,11,12
4	Source Quench	0
5	Redirect	0,1,2,3
8	Echo Request	0
9	Router Advertisement	0
10	Router Solicitations	0

Código IPv4

0,1,2,3,4,5,6,7,8,9,10,11,12

IPv6		
Tipo		**Códigos admitidos**
1	Destination Unreachable	0,1,2,3,4
3	Time Exceeded	0,1
4	Parameter Problem	0,1,2
128	Echo Request	0
129	Echo Reply	0
133	Router Solicitation	0
134	Router Advertisement	0
135	Neighbor Solicitation	0
136	Neighbor Advertisement	0
137	Redirect	0

Código IPv6

0,1,2,3,4

Visítenos en Internet
http://www.brother.com/

Brother Earth

www.brotherearth.com